Havells India

ISMS Communication Policy

Version 1.0

Document Statistics

S. No.	Type of Information	Document Data
1.	Document Title	Havells India ISMS Communication Policy
2.	Document Code	HISMSCP
3.	Date of Release	20th Feb 2023
4.	Document Superseded	
5.	Document Approvers	Mr. Pramod Mundra and Mr. Ramanand Jha
6.	Document Owner	Information Security Head
7.	Documents Author(s)	Mr. Sanjay Roongta and Mr. Neeraj Nagpal

Document Approvers

S. No.	Approver	Approver Designation	Approver Contact
1.	Pramod Mundra	Chief Information Officer (CIO)	Pramod.Mundra@havells.com
2.	Ramanand Jha	Information Security Head	ramanand.jha@havells.com

Document Change Approvals

Version No.	Revision Date	Nature of Change	Date Approved
1.0	NA	Initial Version	18th Feb 2022
1.0	NA	No change	17th Feb 2023

Document Scope

This document shall be applicable to the IT Department and the employees/Third Parties referred henceforth shall include the staff working with IT department and/or handling, processing, and managing information/information assets of Havells.

Document Distribution

The Information Security Head shall distribute this policy to all employees working with IT department and/or handling, processing and managing information/information assets of Havells by uploading it on the intranet/by sharing it via email/as appropriate.

Document Conventions

All statements in the document are mandatory requirements. Failure to observe these requirements may be construed as non-compliance to the policy.

Table of Contents

1. Purpose

The purpose of ISMS Communication Policy is to outline the steps for Havells to use, when communicating information related to security incidents.

1.1 Scope & Audience

This policy shall be applicable to the IT department and the employees/Third Party who deal with Havells' IT and/or handle, process or manage information/information assets of Havells.

1.2 Responsibility

It is the responsibility of the IT Team and respective or concerned business/functional team to implement and maintain the guidelines as defined in the ISMS Communication Policy.

1.3 Enforcement

All Employees and/or Third Party, who deal with Havells' IT and/or handle, process or manage information/information assets of Havells, must comply with this policy. All statements in the document are mandatory requirements. Failure to observe these requirements may be construed as non-compliance to the policy.

a) Non-compliance with this policy shall be dealt with in accordance with the approved management process.

b) Employees and Third Parties who breach this policy shall be subject to disciplinary action.

Requests for deviations from this policy must be documented and managed using the approved process. Any requests for deviations from this policy must be approved in accordance with the Security Exception Management Policy.

1.4 Authority

The Chief Information Officer (CIO) and Information Security Head approves and enforces this policy and mandates processes to monitor and ensure compliance to this policy.

2. Policy

The intent of this policy is to state the communication procedure that shall be followed within Havells India to communicate information security related events to the relevant stakeholders.

2.1 Responsibility

The CIO/Information Security Head/ Head of IT shall be responsible and accountable for the communication procedure. The Information security team can be consulted for communication of any information security related events at Havells. Concerned employees shall be informed of major security related events, which may have a severe impact.

3. Internal and External Communication

3.1 Internal Communication

CIO/Information Security Head/Head of IT shall be responsible for ensuring:

a) That lessons learnt from nonconformities and incidents and subsequent security investigations are communicated to the relevant stakeholders;

b) Reports are presented at the management review meetings.

The ISMS matrix described below defines the context, event, responsibility for communication and what needs to be communicated. The mode of communications for Havells shall be through any electronic communication/verbal as applicable.

Context	Event	Content to be communicated	Communicated by	Communicated to
Roles and responsibilities under ISMS	Change in responsibilities for a particular ISMS role	Communication of the changed responsibilities and changed role expectation as a result of the addition of new responsibility	CIO/Information Security Head/head of IT/Vertical HOD (in case of changes related to Information Security roles)	Information Security Team
	In case of change in personnel to whom an ISMS role had been allocated	Scheduled meetings' content (Minutes of Meeting/ any such document or meeting agenda)	CIO/Information Security Head/head of IT/Vertical HOD (in case of changes related to Information Security roles)	Information Security Team
ISMS policy	Change or revision in ISMS policy	Scheduled meetings' content, "For your information" mailer with the relevant	Information Security Head	Information Security Team

Context	Event	Content to be communicated	Communicated by	Communicated to
		updated information of ISMS policy		
Information Security Incident	Major IT information security incident notification	"For your information mailer" about the incident and the affected system and services and any additional precautionary measures	Information Security Head	Relevant stakeholders, Information Security Team, Vendors (as appropriate)
	Major non-IT information security incident notification		CIO/Head of IT	
	Detection of an Information Security incident	Details of the incident and the time and location of detection.	Users, IT support teams, SOC	Information Security Head/ Information Security Team/ IT team
	Detection of a non-IT Information Security incident	Details of the incident and the time and location of detection.	Users, IT support teams, SOC	Information Security Head / Admin Head/Functional Lead/CIO/Head of IT
Information security vulnerabilities	Identification of any Information security control lapse or weakness	Email describing details and description of the information security weakness identified along with the systems affected	Users /IT Teams / SOC	Information Security Head, Functional lead/ SOC/IT team
Information Security Awareness Communication	All communication related to information security awareness	Awareness material	Information Security Team/Information Security Head/IT team	Relevant employees

3.2 External Communication

All external communications to Havells that relate to Information security will be sent to the designated authority for review & dissemination as appropriate, which includes:

a) Changes in Havells' Information Security Policies, pertaining to Third Party;
b) New, amendments or pending changes to legislation;
c) Proposed changes to Third Party contracts, terms & conditions, NDAs that affect information security requirements.

Context	Event	Content to be communicated	Communicated by
ISMS policy (wherever applicable)	Change or revision in ISMS policy	Revised ISMS policy where applicable	Information Security Head/CIO/ head of IT / concerned functional head
Information Security Incident	Major IT information security incident notification	“For your information mailer” about the incident and the affected system and services and any additional precautionary measures	Information Security Head/CIO / Head of IT